

Z_4 -linear Hadamard and extended perfect codes¹

D. S. Krotov

Sobolev Institute of Mathematics, Russia

Abstract

If $N = 2^k \geq 16$ then there exist exactly $\lfloor (k-1)/2 \rfloor$ pairwise nonequivalent Z_4 -linear Hadamard $(N, 2N, N/2)$ -codes and $\lfloor (k+1)/2 \rfloor$ pairwise nonequivalent Z_4 -linear extended perfect $(N, 2^N/2N, 4)$ -codes. A recurrent construction of Z_4 -linear Hadamard codes is given.

Key words: Hadamard Codes, Perfect Codes, Z_4 -Linear Codes

1 Introduction

Certain of known nonlinear binary codes such as Kerdock, Preparata, Goethals, Delsarte-Goethals codes are represented by use of a map $\{0, 1, 2, 3\} \rightarrow \{0, 1\}^2$ as linear codes over the alphabet $\{0, 1, 2, 3\}$ with modulo 4 operations (see [1,2]) (following [2], we will use the map $0 \rightarrow 00, 1 \rightarrow 01, 2 \rightarrow 11, 3 \rightarrow 10$). Codes represented in such a manner are called Z_4 -linear.

Our research is devoted to Z_4 -linear Hadamard $(N, 2N, N/2)$ -codes and Z_4 -linear extended perfect $(N, 2^N/2N, 4)$ -codes. Linear in the ordinary sense $(N, 2N, N/2)$ -code and $(N, 2^N/2N, 4)$ -code exist for every $N = 2^k$ and unique up to equivalence. These codes are first order Reed-Muller code and extended Hamming code respectively. In [2] it was shown that the first order Reed-Muller codes are Z_4 -linear and the Hamming code of length N is Z_4 -linear if and only if $N \leq 16$. Also in [2] a Z_4 -linear $(N, 2^N/2N, 4)$ -code was presented

Email address: krotov@math.nsc.ru (D. S. Krotov).

¹ This is a reprint of: — In *Proc. the Int. Workshop on Coding and Cryptography WCC'2001*, pages 329–334, Paris, France, January 2001. *Electron. Notes Discrete Math.*, 6: 107–112, 2001. DOI: 10.1016/S1571-0653(04)00161-1

in a cyclic form for every $N = 2^k$. The aim of our research is a full up to equivalence classification of Z_4 -linear $(N, 2N, N/2)$ - and $(N, 2^N/2N, 4)$ -codes. The results on extended perfect $(N, 2^N/2N, 4)$ -codes are proved in [3]. (A complete classification of the Z_4 -linear Hadamard codes can be found in [PRV2006]; for more references on the subject, see arXiv:0710.0198 – transl. rem.)

2 Main definitions and facts

Let E^N be the set of all binary words of length N . *Hamming distance* $d(x, y)$ between x and y from E^N is the number of positions in which x and y differ. Binary (N, K, d) -code is a subset C of E^N such that $|C| = K$ and $d(c_1, c_2) \geq d$ for every different $c_1, c_2 \in C$. If $c_1 \oplus c_2 \in C$ for every $c_1, c_2 \in C$ then C is *linear code*.

Let Z_4^n be the set of n -words over the alphabet $Z_4 = \{0, 1, 2, 3\}$ with (mod 4) addition and multiplication by a constant. An additive subgroup of Z_4^n is called a *quaternary code*. Two quaternary codes are *equivalent* if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates.

Lee weight $wt_L(a)$ of $a \in Z_4^n$ is the rational sum of the Lee weights of its coordinates, where $wt_L(0) = 0$, $wt_L(1) = wt_L(3) = 1$ and $wt_L(2) = 2$. The weight function wt_L defines *Lee distance* $d_L(a, b) \stackrel{\text{def}}{=} wt_L(b - a)$ on Z_4^n .

We say that a quaternary code \mathcal{C} is a *quaternary distance d code of length n* or \mathcal{C} is a $(n, |\mathcal{C}|, d)_4$ -code if $\mathcal{C} \subseteq Z_4^n$ and $d_L(a, b) \geq d$ for every different $a, b \in \mathcal{C}$.

Every quaternary code \mathcal{C} can be defined by a *generating matrix* of the form

$$G = \begin{bmatrix} G_1 \\ 2G_2 \end{bmatrix}, \quad (1)$$

where G_1 is a Z_4 -matrix of size $k_1 \times n$, G_2 is a Z_2 -matrix of size $k_2 \times n$, $|\mathcal{C}| = 2^{2k_1+k_2}$, and every $c \in \mathcal{C}$ can be represented in form

$$c = (v_1, v_2) \begin{bmatrix} G_1 \\ 2G_2 \end{bmatrix} \pmod{4}, \quad v_1 \in Z_4^{k_1}, \quad v_2 \in Z_2^{k_2}.$$

The code \mathcal{C} defined by generating matrix (1) is an elementary Abelian group of type $4^{k_1}2^{k_2}$. We say in this case that \mathcal{C} is a code of type $4^{k_1}2^{k_2}$.

Every quaternary code \mathcal{C} of type $4^{k_1}2^{k_2}$ can be defined also by a *check matrix*

$$A = \begin{bmatrix} A_1 \\ 2A_2 \end{bmatrix}$$

by condition

$$Ac^T = 0 \quad \text{for all } c \in \mathcal{C},$$

where A_1 is a Z_4 -matrix of size $(n - k_1 - k_2) \times n$ and A_2 is a Z_2 -matrix of size $k_2 \times n$. The code \mathcal{C}^* with generator matrix A is called the *dual* to \mathcal{C} .

Let two maps $\beta(c), \gamma(c) : Z_4 \rightarrow Z_2$ be defined by

$$\begin{array}{ccc} c & \beta(c) & \gamma(c) \\ 0 & 0 & 0 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \\ 3 & 1 & 0 \end{array},$$

and let them be extended coordinate-wise to maps from Z_4^n to Z_2^n . The *Gray map* $\phi : Z_4^n \rightarrow E^{2n}$ is defined by (cf.[2])

$$\phi(c) = (\beta(c), \gamma(c)), \quad c \in Z_4^n.$$

So the i -th coordinate of a word $c \in Z_4^n$ corresponds to i -th and $(i + n)$ -th coordinates of the binary word $\phi(c)$. In such a manner a binary code of length $2n$ corresponds to any quaternary code of length n . A binary code C of length $2n$ is called Z_4 -linear if there exist a quaternary code \mathcal{C} and a permutation π of $2n$ coordinate such that $C = \pi(\phi(\mathcal{C}))$.

Two binary codes C and C' of length N are called *equivalent* if there exist a word $y \in E^N$ and a permutation π of order N such that $C = \pi(C' \oplus y)$. If quaternary codes \mathcal{C} and \mathcal{C}' are equivalent, then related binary codes $\phi(\mathcal{C})$ and $\phi(\mathcal{C}')$ are also equivalent.

The following lemma follows immediately from definitions of distances $d(\cdot, \cdot)$, $d_L(\cdot, \cdot)$ and the mapping $\phi(\cdot)$

Lemma 1 [2] *The mapping ϕ is an isometry from Z_4^n with Lee distance to E^{2n} with Hamming distance. In other words*

$$d_L(a, b) = d(\phi(a), \phi(b)), \quad a, b \in Z_4^n.$$

3 Construction

Let r_1 and r_2 be nonnegative integers. Let the matrix A^{r_1, r_2} consist of lexicographically ordered columns z^T , $z \in \{1\} \times \{0, 1, 2, 3\}^{r_1} \times \{0, 2\}^{r_2}$. For example

$$A^{0,0} = [1], \quad A^{0,1} = \begin{bmatrix} 11 \\ 02 \end{bmatrix},$$

$$A^{1,0} = \begin{bmatrix} 1111 \\ 0123 \end{bmatrix}, \quad A^{0,2} = \begin{bmatrix} 1111 \\ 0022 \\ 0202 \end{bmatrix},$$

$$A^{1,1} = \begin{bmatrix} 11 & 11 & 11 & 11 \\ 00 & 11 & 22 & 33 \\ 02 & 02 & 02 & 02 \end{bmatrix}, \quad A^{0,3} = \begin{bmatrix} 11 & 11 & 11 & 11 \\ 00 & 00 & 22 & 22 \\ 00 & 22 & 00 & 22 \\ 02 & 02 & 02 & 02 \end{bmatrix},$$

$$A^{2,0} = \begin{bmatrix} 1111 & 1111 & 1111 & 1111 \\ 0000 & 1111 & 2222 & 3333 \\ 0123 & 0123 & 0123 & 0123 \end{bmatrix}.$$

For all integers $r_1, r_2 \geq 0$ define the dual quaternary codes \mathcal{H}^{r_1, r_2} and \mathcal{C}^{r_1, r_2} :

$$\mathcal{H}^{r_1, r_2} \stackrel{\text{def}}{=} \{(v_1, v_2)A^{r_1, r_2} : v_1 \in Z_4^{r_1+1}, v_2 \in Z_2^{r_2}\},$$

$$\mathcal{C}^{r_1, r_2} \stackrel{\text{def}}{=} \{c \in Z_4^{2^{r_1+r_2}} : A^{r_1, r_2}c^T = 0\}.$$

The matrix A^{r_1, r_2} is a generator matrix for \mathcal{H}^{r_1, r_2} and a check matrix for \mathcal{C}^{r_1, r_2} .

Let $n = 2^{2r_1+r_2}$.

Theorem 2 a) *The set \mathcal{H}^{r_1, r_2} is a quaternary $(n, 4n, n)_4$ -code;*
b) *the set \mathcal{C}^{r_1, r_2} is a quaternary $(n, 4^n/4n, 4)_4$ -code.*

Let $H^{r_1, r_2} \stackrel{\text{def}}{=} \phi(\mathcal{H}^{r_1, r_2})$, $C^{r_1, r_2} \stackrel{\text{def}}{=} \phi(\mathcal{C}^{r_1, r_2})$ and let $N \stackrel{\text{def}}{=} 2n = 2^{2r_1+r_2+1}$. By Lemma 1, Theorem 2 means that

Corollary 3 a) *The set H^{r_1, r_2} is a binary $(N, 2N, N/2)$ -code;*
b) *the set C^{r_1, r_2} is a binary $(N, 2^N/2N, 4)$ -code.*

4 The nonexistence of $(n, 4n, n)_4$ - and $(n, 4^n/4n, 4)_4$ -codes that are nonequivalent to the constructed codes

Theorem 4 a) Let the set $\mathcal{H} \subset Z_4^n$ be a $(n, 4n, n)_4$ -code of type $4^{r_0}2^{r_2}$. Then $n = 2^{2(r_0-1)+r_2}$, $r_0 > 0$, and \mathcal{H} is equivalent to \mathcal{H}^{r_0-1, r_2} .
b) Let the set $\mathcal{C} \subset Z_4^n$ be a $(n, 4^n/4n, 4)_4$ -code of type $4^{n-r_0-r_2}2^{r_2}$. Then $n = 2^{2(r_0-1)+r_2}$, $r_0 > 0$, and \mathcal{C} is equivalent to \mathcal{C}^{r_0-1, r_2} .

Corollary 5 a) Each Z_4 -linear $(N, 2N, N/2)$ -code is equivalent to some code H^{r_1, r_2} , $2^{2r_1+r_2+1} = N$.
b) Each Z_4 -linear $(N, 2^N/2N, 4)$ -code is equivalent to some C^{r_1, r_2} , $2^{2r_1+r_2+1} = N$.

5 The nonequivalence of H^{r_1, r_2}

If H is a binary code of length N then

$$\text{kernel}(H) \stackrel{\text{def}}{=} \{x \in E^N : x \oplus H = H\}.$$

The proof of pairwise nonequivalency of the codes H^{r_1, r_2} is based on the following fact.

Proposition 6 If binary codes H_1 and H_2 are equivalent then $|\text{kernel}(H_1)| = |\text{kernel}(H_2)|$.

The following two propositions establish the cardinalities of kernels of the codes H^{r_1, r_2} .

Proposition 7 The codes H^{0, r_2} and H^{1, r_2} are linear. Hence $\text{kernel}(H^{0, r_2}) = H^{0, r_2}$ and $\text{kernel}(H^{1, r_2}) = H^{1, r_2}$.

Proposition 8 Let $r_1 > 1$. Then $|\text{kernel}(H^{r_1, r_2})| = 2^{r_1+r_2+2}$ and the code H^{r_1, r_2} is nonlinear.

The following theorem stems from Propositions 6-8.

Theorem 9 Let $2r_1 + r_2 = 2r'_1 + r'_2$ and $r_1 \geq 2$. Then the codes H^{r_1, r_2} and $H^{r'_1, r'_2}$ are equivalent if and only if $r_1 = r'_1$.

From Theorem 9, using Corollary 5, we have

Theorem 10 If $N = 2^k \geq 8$ then there exist exactly $\lfloor (k-1)/2 \rfloor$ pairwise nonequivalent Z_4 -linear Hadamard codes of length N .

6 The nonequivalence of C^{r_1, r_2}

If N is even and $C \subset E^N$ then

$$\text{even}(C) \stackrel{\text{def}}{=} \{(c_0, c_2, \dots, c_{N-2}) \in E^{N/2} \mid (c_0, 0, c_2, 0, \dots, c_{N-2}, 0) \in C\},$$

$$\text{odd}(C) \stackrel{\text{def}}{=} \{(c_1, c_3, \dots, c_{N-1}) \in E^{N/2} \mid (0, c_1, 0, c_3, \dots, 0, c_{N-1}) \in C\}.$$

We use these definitions and the following proposition for the induction step.

Proposition 11 *It is true that*

- a) $\text{even}(C^{r_1, r_2}) = \text{odd}(C^{r_1, r_2}) = C^{r_1, r_2-1}$ for every $r_1 \geq 0$ and $r_2 > 0$;
- b) $\text{even}(C^{r_1, 0}) = \text{odd}(C^{r_1, 0}) = C^{r_1-1, 1}$ for every $r_1 > 0$.

Let the maximal number of linearly independent vectors from a binary code C be noted $\text{rank}(C)$.

The proof of pairwise nonequivalence of C^{r_1, r_2} is based on the following fact.

Proposition 12 *If binary codes C_1 and C_2 are equivalent then $\text{rank}(C_1) = \text{rank}(C_2)$.*

Proposition 13 *For all integers $r_1 \geq 0$, $r_2 \geq 0$*

$$\text{rank}(C^{r_1, r_2}) \leq N - r_1 - r_2 - 1, \quad (2)$$

where $N = 2^{2r_1+r_2+1}$ is the length of code C^{r_1, r_2} .

It is straightforward that (2) is tight for $r_1 = r_2 = 1$ and $r_1 = 0, r_2 = 4$:

Proposition 14 *It is true that $\text{rank}(C^{1,1}) = 13$ and $\text{rank}(C^{0,4}) = 27$.*

Using Proposition 11 it can be established by induction that (2) is tight for every $r_1, r_2 \geq 1$ or $r_1 \geq 0, r_2 \geq 4$:

Lemma 15 *Let $r_1 \geq 1, r_2 \geq 0$ be integers such that $2r_1 + r_2 \geq 3$ and $(r_1, r_2) \neq (0, 3)$. Then*

$$\text{rank}(C^{r_1, r_2}) = 2^{2r_1+r_2+1} - r_1 - r_2 - 1.$$

Remark 16 *The set $C^{0,3}$ is a linear code and $\text{rank}(C^{0,3}) = 11$.*

Theorem 17 *Let $2r_1 + r_2 = 2r'_1 + r'_2 \geq 3$. Then the codes C^{r_1, r_2} and $C^{r'_1, r'_2}$ are equivalent if and only if $r_1 = r'_1$ (equivalently, $r_2 = r'_2$).*

By Corollary 3 and Corollary 5 we have

Theorem 18 *If $N = 2^k \geq 16$ then there exist exactly $\lfloor (k+1)/2 \rfloor$ pairwise nonequivalent Z_4 -linear extended perfect distance 4 codes of length N .*

7 Recurrent construction of codes \mathcal{H}^{r_1, r_2}

Let \mathcal{H} be a quaternary $(n, 4n, n)_4$ -code, $\mathcal{R}' = \{00\dots 0, 22\dots 2\}$ be the quaternary $(n, 2, 2n)_4$ -code, and $\mathcal{R}'' = \{00\dots 0, 11\dots 1, 22\dots 2, 33\dots 3\}$ be the quaternary repetition $(n, 4, n)_4$ -code. Let

$$\mathcal{H}' \stackrel{\text{def}}{=} \{(a, a+b) : a \in \mathcal{H}, b \in \mathcal{R}'\}, \quad (3)$$

$$\mathcal{H}'' \stackrel{\text{def}}{=} \{(a, a+b, a+2b, a+3b) : a \in \mathcal{H}, b \in \mathcal{R}''\}.$$

Remark 19 *The construction (3) is a particular case of well known Plotkin $(u, u+v)$ -construction.*

Proposition 20 *The set \mathcal{H}' is a quaternary $(2n, 4(2n), 2n)_4$ -code. If \mathcal{H} is equivalent to \mathcal{H}^{r_1, r_2} then \mathcal{H}' is equivalent to \mathcal{H}^{r_1, r_2+1} . If $\mathcal{H} = \mathcal{H}^{0, r_2}$ then $\mathcal{H}' = \mathcal{H}^{0, r_2+1}$.*

Proposition 21 *The set \mathcal{H}'' is a quaternary $(4n, 4(4n), 4n)_4$ -code. If $\mathcal{H} = \mathcal{H}^{r_1, r_2}$ then $\mathcal{H}'' = \mathcal{H}^{r_1+1, r_2}$.*

Using Propositions 20 and 21 one can construct every code \mathcal{H}^{r_1, r_2} starting with the trivial code $\mathcal{H}^{0,0} = \{0, 1, 2, 3\}$.

A recurrent construction of the class of codes \mathcal{C}^{r_1, r_2} can be found in [3].

References

- [1] Nechaev, A. A. Kerdock code in a cyclic form // Diskretnaya Matematika. 1989. Vol. 1, 4. P.123–139. English transl.: Discrete Mathematics and Applications. 1991. Vol. 1, 4. P. 365–384.
- [2] Hammons, A. R., Jr, Kumar, P. V., Calderbank, A. R., Sloane, N. J. A., Solé, P. The Z_4 -linearity of Kerdock, Preparata, Goethals, and related codes // IEEE Trans. Inform. Theory. 1994. Vol. 40, 2. P. 301–319. DOI: 10.1109/18.312154
- [3] Krotov, D. S. Z_4 -linear perfect codes // Diskretn. Anal. Issled. Oper. Ser.1. 2000. Vol. 7, 4. P. 78–90. English transl: arXiv:0710.0198
- [PRV2006] K. T. Phelps, J. Rifà, and M. Villanueva. On the additive (Z_4 -linear and non- Z_4 -linear) Hadamard codes: Rank and kernel. *IEEE Trans. Inf. Theory*, 52(1):316–319, 2006. DOI: 10.1109/TIT.2005.860452.